IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

*Richmond Division*

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | ) | |
| | ) | |
| v. | ) | CRIMINAL NO. 3:19-CR-130-MHL |
| | ) | |
| OKELLO T. CHATRIE, | ) | |
| | ) | |
| Defendant. | ) | |

**GOVERNMENT'S RESPONSE IN OPPOSITION TO**
**DEFENDANT'S MOTION FOR SUPPRESSION**

When someone robbed the Call Federal Credit Union in Chesterfield, Virigina, Google was a witness. Defendant Okello T. Chatrie had chosen to have Google keep a record of where he went with his cell phone in order for Google to provide him with location-based services. As a result, evidence of the defendant's presence at the bank robbery was stored in a database that Google accesses freely to provide services to its users and advertisers. A Virginia magistrate determined that there was probable cause to believe that Google possessed evidence of the robbery, and he issued a geofence search warrant.

The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, over a one-hour interval, within 150 meters of the site of the bank robbery. Pursuant to the warrant, Google produced location information over a two-hour interval of three subsequently identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals. From this information, investigators identified the defendant and solved the robbery.

In his post-hearing brief, the defendant continues to argue that this evidence should be

suppressed, but this Court should deny the defendant's motion to suppress for three separate and independent reasons. *See* Def.'s Post-Hearing Mot. To Suppress, ECF No. 203, (hereinafter, "Def. Post-Hr'g Suppl. Br."). First, the government did not conduct a search under the Fourth Amendment when it obtained this location information from Google. Second, the geofence warrant complied with the Fourth Amendment, as it was based on probable cause and specified its object with particularity. Third, suppression is inappropriate because investigators relied on the warrant in good faith.

## I. STATEMENT OF FACTS

### *A. The Robbery and the Geofence Warrant*

At approximately 4:50 pm on May 20, 2019, a then-unknown male entered the Call Federal Credit Union in Midlothian, Virginia. *See* Geofence Search Warrant, Gov't Ex. 2, at 6 (hereinafter, "Gov't Ex. 2")[1]; Motion to Suppress Hearing Transcript, ECF Nos. 101, 102, at 608 (hereinafter, "Suppression Hr'g Tr."). With his right hand, the robber held a cell phone to his face and appeared to be speaking to someone. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608. He approached a teller and presented a note that read, in part, "I got your family as hostage and I know where you live, If you or your coworker alert the cops or anyone your family and you are going to be hurt. . . . I need at least 100k." Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. After the teller replied that she did not have access to that amount of money, the robber pulled out a silver and black firearm. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609. After first forcing everyone to the ground at gunpoint, the robber escorted the manager and others to the back of the business where the vault was located. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 608-09. The robber forced the manager to open the safe

[1] Page numbers for Government Exhibit 2 refers to the numbering in red at the bottom of each page. Such numbering is consistent where an exhibit of the United States has red numbering at the bottom.

and place $195,000 into a bag. Gov't Ex. 2 at 6. The robber then fled towards a church west of the bank. Gov't Ex. 2 at 6; Suppression Hr'g Tr. 609-10.

Federal Bureau of Investigation Task Force Officer ("FBI TFO") Josh Hylton responded to the scene to investigate. Suppression Hr'g Tr. 607. From the fact that the robber had carried a phone, FBI TFO Hylton knew that there was a possibility that the robber might have had a lookout or a driver nearby. Suppression Hr'g Tr. 610.

FBI TFO Hylton also knew that Google could have data that would show the robber was in the area at the time of the robbery. Suppression Hr'g Tr. 610. On three prior occasions, FBI TFO Hylton had obtained geofence warrants directed to Google. Suppression Hr'g Tr. 603. Moreover, he had consulted with prosecutors prior to obtaining the geofence warrants. Suppression Hr'g Tr. 604. One was issued by a United States Magistrate Judge, and two were issued by Virginia state judges. Suppression Hr'g Tr. 603-04. In seeking these warrants, he had never been told that geofence warrants were not legal. Suppression Hr'g Tr. 604-05.

On June 14, 2019, FBI TFO Hylton sought and obtained a geofence warrant from the Chesterfield Circuit Court of Virginia. *See* Gov't Ex. 2. His statement of probable cause began by describing the facts of the robbery, including that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone. Gov't Ex. 2 at 6. The statement then explained why there was reason to believe that Google would have evidence pertaining to the robbery. Gov't Ex. 2 at 7. Among other facts, the statement disclosed: (1) that as of 2013, 56% of cell phones were smartphones; (2) that "[n]early every" Android phone "has an associated Google account"; (3) that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (4) that Google collects location information from non-Android smartphones if the devices are "registered to a Google account and the user has

location services enabled." Gov't Ex. 2 at 7. Magistrate David Bishop issued the geofence warrant upon a finding of probable cause. *See* Gov't Ex. 2 at 8.

The geofence warrant specified a target geographical area, identified as a circle of radius 150 meters around a specific latitude and longitude point west of the bank, such that the circle covered both the bank and the place where the robber parked. Gov't Ex. 2 at 5; Suppression Hr'g Tr. 523. It authorized disclosure of location information over a two-hour interval (from 3:50 pm to 5:50 pm) from accounts associated with devices within this target area at some point during a one-hour interval that included the robbery (from 4:20 pm to 5:20 pm). Gov't Ex. 2 at 4-5. The warrant also authorized disclosure of specified customer identity information associated with these accounts, including user name and email address. Gov't Ex. 2 at 4-5.

The warrant authorized this disclosure through a three-step process that enabled law enforcement to "narrow down" the information disclosed by Google and thus obtain less than the maximum amount of information covered by the warrant. Gov't Ex. 2 at 4-5. The warrant directed that in the first step, Google was to disclose anonymized location for devices present in the target area during the hour of the robbery, but not the identity information associated with the devices. Gov't Ex. 2 at 4. In particular, the warrant directed that Google disclose "a numerical identifier for the account, the type of account, time stamped location coordinates and that data source that this information came from if available." Gov't Ex. 2 at 4.

In the second step, law enforcement was to review the anonymized location information produced by Google and identify the accounts of interest, and Google was then to disclose location information for those accounts over the full two-hour interval, both within and outside of the target area, but again without disclosing user identity information. Gov't Ex. 2 at 4-5. In the third step, law enforcement was to identify accounts that remained of interest, and Google was to disclose

user name and other specified subscriber identity information for those accounts. Gov't Ex. 2 at 5.

Investigators followed this three-step process in executing the warrant. Suppression Hr'g Tr. 533-50. In the first phase, Google provided 209 data points concerning 19 accounts (including 38 points from the defendant's account), all within the 150 meter circle and during the hour of the bank robbery. *See* FBI Cellular Analysis Survey Team, Gov't Ex. 1, at 20, 22 (hereinafter, "FBI CAST Report"); Suppression Hr'g Tr. 534-35; *see also* Sealed PDF of Raw Data, Def. Ex. 3. For each data point, Google produced an account ID, date and time, latitude and longitude coordinate, source of information (wi-fi or GPS), and "map display radius." *See* FBI CAST Report at 17-22. "Map display radius" is a measure of Google's confidence in the accuracy of its location information; Google's aim is to capture roughly 68% of users within the circle defined by its location estimate and the map display radius. Suppression Hr'g Tr. 213-14; *see also* McGriff Decl. dated Mar. 11, 2020 at ¶¶ 24-25 (ECF No. 96-1), Gov't Ex. 3, (hereinafter, "Gov't Ex. 3").

By reviewing the phase 1 data in conjunction with witness interviews and video surveillance tapes, investigators concluded that the defendant's device likely belonged to the robber. Suppression Hr'g Tr. 549-50.

In the second phase, FBI TFO Hylton initially asked Google for data regarding all 19 accounts, but Google was nonresponsive. Suppression Hr'g Tr. 622; Email Correspondence between FBI TFO Hylton and Google, Gov't Ex. 4 at 4. Concerned about the dangerousness of the situation, FBI TFO Hylton called Google, and he ultimately narrowed the second-stage production to nine accounts. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google produced two hours of location data for each of these accounts—a total of 680 data points, including 94 data points for the defendant's account with a device ID ending in 5659. FBI CAST Report at 26.

In the third phase, FBI TFO Hylton directed Google to disclose subscriber information for three accounts, including the account of the defendant. Suppression Hr'g Tr. 543. This information included the defendant's email address. Suppression Hr'g Tr. 544.

Location History information is the only information stored by Google that can be responsive to a geofence warrant because it is the only information stored by Google that is associated with specific users and sufficiently granular to be responsive. *See* Gov't Ex. 3 at ¶ 20; Suppression Hr'g Tr. 378-79. To identify responsive information, Google runs a computation against all stored Location History coordinates to determine which ones match the geofence parameters. *See* Gov't Ex. 3 at ¶ 20. It would be technically possible for Google to index its Location History database by user location rather than user accounts. Suppression Hr'g Tr. 402-03.

*B. The Defendant's Google Account*

On August 20, 2017, the defendant created the email account Okellochatrie55@gmail.com. McGriff Decl. dated Aug. 7, 2020 at ¶ 2 (ECF No. 171-1) & Gov't Ex. 3c at Exhibit A (hereinafter, Gov't Ex. 3c). At that time, he agreed to Google's terms of service. Suppression Hr'g Tr. 382. Those terms specified that "[b]y using our Services, you agree that Google can use such data in accordance with our privacy policies." See Google Terms of Service last modified October 25, 2017 at 3, Gov't Ex. 5a, (hereinafter, "Gov't Ex. 5a"). [2]

On July 9, 2018, the defendant opted in to Google's storage of his Location History. Gov't Ex. 3c at ¶ 5 & Exhibit B. Google Location History allows users "to keep track of locations they

[2] The terms of service available at that time are also available at https://policies.google.com/terms/archive/20140414. The best evidence of Google's privacy policy and terms of service is online. Suppression Hr'g Tr. 386.

have visited while in possession of their compatible mobile devices." Gov't Ex. 3 at ¶ 4. Google uses Location History to provide location-based services to users: for example, users can obtain "recommendations based on places they have visited, get help finding their phones, and receive real-time traffic updates about their commutes." Gov't Ex. 3 at ¶ 6; Suppression Hr'g Tr. 292, 347.

Google also uses Location History for advertising purposes. Gov't Ex. 3 at ¶¶ 5, 14; Suppression Hr'g Tr. 196-98, 561. It infers users' interests from where they visit, and it uses that "semantic location information" to target advertising to users. Gov't Ex. 3 at ¶¶ 5, 14. Google also targets ads to users based on their proximity to a particular business. Suppression Hr'g Tr. 198. In addition, Google uses location information to measure "store visit conversions"—how many customers who saw a particular ad went on to visit a relevant store. Gov't Ex. 3 at ¶ 14; Suppression Hr'g Tr. 196-97. Although Google does not share a user's Location History directly with advertisers, it does share with advertisers store visit conversion information that it derives from Location History. Suppression Hr'g Tr. 196-97, 561.

The majority of Google users decline to opt in to Location History. Suppression Hr'g Tr. 351. In 2019, approximately one-third of active Google users had Location History enabled. Gov't Ex. 3 at ¶ 13; Suppression Hr'g Tr. 387.

A Google user may review, edit, or delete Location History information. Gov't Ex. 3 at ¶ 15; Suppression Hr'g Tr. 321, 388, 416. Deletion takes place nearly immediately. Suppression Hr'g Tr. 416. Deleted Location History information is not retained at all, even in anonymized form. Suppression Hr'g Tr. 321. A Google user may also stop collection of Location History information. Suppression Hr'g Tr. 416. Stopping collection can be accomplished through any of three paths: settings on any App that uses Location History, device-level settings, or through the

myactivity.google.com website. Suppression Hr'g Tr. 340-41.

Opting in to storage of Location History is not the only step a user must take in order for Google to store the user's Location History. Gov't Ex. 3 at ¶¶ 7-11. As Location History Product Manager Marlo McGriff explained, Location History "functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it." Gov't Ex. 3 at at ¶ 10.[3]

When the defendant opted in to Location History on July 9, 2018, a user could not opt in to storage of Location History without following Google's "supported consent flow," which is "the steps and consent text necessary to opt in" to its service. Gov't Ex. 3c at ¶ 6. If a user attempted to opt in using an unsupported consent flow, the process would not be successful. Suppression Hr'g Tr. 297. Under the supported consent flow for Location History on July 9, 2018, Google presented the user with the following text:

> **Location History**
>
> Saves where you go with your devices
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

Gov't Ex. 3c at ¶ 7.

[3] In his testimony at the suppression hearing, McGriff affirmed that he stood by his affidavits. Suppression Hr'g Tr. 376.

Along with this text, Google presented an expansion arrow to the user that the user could tap to obtain additional information about Location History. Gov't Ex. 3c at ¶ 8. This expanded Location History text stated:

> **Location History**
>
> Saves where you go with your devices
>
> Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.
>
> If you use your device without an internet connection, your data may be saved to your account once you return online.
>
> Not all Google services save this data to your account.
>
> This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

Gov't Ex. 3c at ¶ 8.

Regardless of the Application or service a user was using, a user could not opt in to Location History on July 9, 2018, without encountering this consent flow text and tapping "TURN ON." Gov't Ex. 3c at ¶¶ 10-11.

Defense expert Spencer McInvaille determined that he could not "replicate the opt-in process [for Location History] Mr. Chatrie would have seen." McInvaille Suppl. Report, Def. Ex. 7, at 1 (hereinaifter, "Def. Ex. 7"); Suppression Hr'g Tr. 152. From his analysis of the defendant phone, McInvaille believed that the defendant installed Google Assistant shortly before he opted

in to Location History. Suppression Hr'g Tr. 76. McInvaille opined that the defendant had used Google Assistant to activate Location History. Suppression Hr'g Tr. 79.

McInvaille then looked for publicly available information regarding past use of Google Assistant to opt in to Location History. Def. Ex. 7 at 1; Suppression Hr'g Tr. 82. He found three examples, but only his third came from the time frame when the defendant opted in to Location History. Def. Ex. 7 at 1-4. His first example is an article that appeared at qz.com on January 24, 2018, nearly six months before the defendant opted in to Location History. Def. Ex. 7 at 1; Suppression Hr'g Tr. 220. That article includes a screenshot showing some opt-in language for Location History, but the language shown does not follow the supported consent flow required by Google to opt-in on July 9, 2018. Def. Ex. 7 at 1. For example, rather than saying "Saves where you go with your devices", it says "Creates a private map of where you go with your signed-in devices." Def. Ex. 7 at 1.

Second, McInvaille found an Oracle report dated September 2018. Def. Ex. 7 at 2; Oracle Report dated September 2018, Def. Ex. 11 at 4 (hereinafter, "Def. Ex. 11"). The Oracle report also includes screenshots capturing some opt-in language for Location History, but it does not identify when its screenshot were taken, and the language from the screenshots again does not follow the supported consent flow required by Google to opt in on July 9, 2018. Def. Ex. 7 at 2; Def. Ex. 11 at 4. For example, like the qz.com article, the screenshot states: "Creates a private map of where you go with your signed-in devices." Def. Ex. 7 at 2; Def. Ex. 11 at 4.

Third, McInvaille found a report from the Norwegian Consumer Council with screenshots taken approximately contemporaneously with when the defendant opted in to Location History. Def. Ex. 7 at 3-4. In particular, the Norwegian reports includes screenshots taken on July 2 and August 9, 2018. *Id.* The screenshots in the Norwegian report are consistent with the supported

consent flow set forth by McGriff: every word of the supported consent flow set forth by McGriff is visible in the Norwegian screenshots. Gov't Ex. 3c at ¶¶ 7, 8; Def. Ex. 7 at 3-4. McInvaille believed that the Norwegian report captures "the true depiction of the opt-in process." Suppression Hr'g Tr. 100.

The Google Assistant process varied based on a user's previous use of Google's products and services. Suppression Hr'g Tr. 415. The screenshots from the Norwegian report showed opt-in text for Location History bundled with opt-in language for Device Information and Voice and Audio Activity. Def. Ex. 7 at 3-4. However, a user who had previously consented to Device Information and Video and Audio Activity would see only Location History. Suppression Hr'g Tr. 335. The record does not indicate whether the defendant opted in to any other Google services at the time he opted in to Location History.

Google's Privacy Policy provided further information to Google users regarding Google's storage and use of location information. Google Privacy Policy effective January 22, 2019, Gov't Ex. 5 (hereinafter, "Gov't Ex. 5"). The Privacy Policy in effect on the date of the robbery—May 20, 2019—included the following:

> We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you. . . .
>
> The types of location data we collect depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices. . . .
>
> We use the information we collect in existing services to help us develop new ones. . . .
>
> For example, you can turn on Location History if you want traffic predictions for your daily commute.

Gov't Ex. 5 at 4-6, 9. The Privacy Policy also explained to users multiple mechanisms for deleting their data, including deleting specific data and deleting data from specific services. Gov't Ex. 5 at 11-12.

## II. ARGUMENT

### A. *The Defendant Had No Reasonable Expectation of Privacy in Two Hours of the Location Information He Disclosed to Google.*

The defendant had no reasonable expectation of privacy in any of the information disclosed by Google pursuant to the geofence warrant. This result is hardly surprising: to obtain location-based services, a user must disclose his location to the service provider. Thus, the government's acquisition of two hours of the defendant's location information is governed by the long-standing principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *United States v. Miller*, 425 U.S. 435, 443 (1976). In addition, the defendant has no reasonable expectation of privacy in his location information under *Carpenter v. United States*, both because *Carpenter* retained the third-party doctrine and because *Carpenter* held only that the government infringes a cell phone owner's reasonable expectation of privacy when it accesses seven days or more of cell phone location information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3, 2220 (2018).

#### 1. The Fourth Amendment does not protect information disclosed to a third party and then conveyed by the third party to the government.

In cases ranging from private conversations to business records, the Supreme Court has repeatedly held that the Fourth Amendment does not protect information revealed to a third party and then conveyed by the third party to the government. This principle applies to statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). It applies to information disclosed to an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36

(1973). It applies to bank records. *See United States v. Miller*, 425 U.S. 435, 443 (1976). It applies to dialed telephone number information. *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1979). It applies to financial records. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984). And in this case, this principle applies to two hours of location information disclosed to Google to obtain location-based services.

In addition to its broad scope, the principle that the government may obtain information revealed to a third party has deep roots. The Supreme Court has recognized that "as early as 1612, . . . Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.'" *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). Similarly, the Court has recognized that it is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixo*n, 418 U.S. 683, 709 (1974). In this case, Google was a witness to the robbery: it had information regarding the bank robbery in a database which it accessed and used to provide services to its users and advertisers. The public had a right to Google's evidence, and the Fourth Amendment did not bar the United States from obtaining that evidence from Google.

2. The defendant voluntarily conveyed his location information to Google.

A closer look at Google's location-based services, its opt-in process, and its agreements with the defendant all confirm what Google told this Court: that Google users "voluntarily choose to save and share [Location History] information with Google." ECF No. 59 at 22.

*a. Google's location-based services*

As an initial matter, the fact that the defendant voluntarily disclosed his location to Google is evident from the nature of the relationship between Google and its users: users provide their

location to Google in order to receive location-based services. Courts often infer that an individual voluntarily disclosed information to a third party based on the nature of the relationship between the individual and the third party. For example, in *Miller*, the Supreme Court did not need to consider Miller's explicit agreements with his bank in order to conclude that he had voluntarily disclosed his financial information. Instead, the Court's conclusion was based on "examin[ing] the nature of the particular documents sought" and concluding that they were "not confidential communications but negotiable instruments to be used in commercial transactions." *Miller*, 425 U.S. at 442.

Google customers disclose their location to Google to obtain services that depend on Google knowing their specific location, such as mapping, traffic updates, help finding their phones, and help with their commutes. Gov't Ex. 3 at ¶ 6; Suppression Hr'g Tr. 347; Gov't Ex. 3c at ¶ 8. Google also uses location information to target advertisements to users, both through users' current location and based on inferences Google draws from Location History. Gov't Ex. 3 at ¶ 5, 14; Suppression Hr'g Tr. 198. In addition, Google uses location information to measure "store visit conversions," which it shares with advertisers. Suppression Hr'g Tr. 196-97.

All of these services demonstrate that Google does more than provide a mere storage service for location information. Based on a user's location, Google provides services that are helpful to the user, like mapping or finding a phone. It uses location information to provide services that are helpful to both the user and other users in the area, like traffic updates. And Google's advertising services employ user location information to benefit the user, the advertiser, and Google itself. In sum, a user of Google's location services does not keep his location private; a user shares location information with Google to obtain location-based services. Because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and

conveyed by him to Government authorities," *Miller*, 425 U.S. at 443, the government did not infringe the defendant's Fourth Amendment interests when it obtained location information he disclosed to Google.

Furthermore, the fact that Google does not normally share a user's specific location directly with additional parties does not affect this analysis. As the Supreme Court stated in *Miller*, the third-party doctrine applies to information disclosed to a third party even "if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. Here, the United States did not infringe the defendant's Fourth Amendment interests because he disclosed his location to Google; the extent to which Google shares that information with others does not change this result.

*b. Google's opt-in process*

The opt-in process necessary for Google to store the defendant's Location History further demonstrates that the defendant voluntarily disclosed his location to Google. Unlike a phone company's collection of cell-site information, Google would not have obtained the defendant's location information during the bank robbery unless the defendant had taken the multiple steps necessary to enable him to share his location with Google. Google saves Location History "only when the user opts into [Location History] as a setting on her Google account, enables the 'Location Reporting' feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it."

Gov't Ex. 3 at at ¶ 10.[4]

McGriff also specified the supported consent flow necessary for the defendant to store his Location History. Gov't Ex. 3c at ¶¶ 7, 8. The text of this consent flow establishes that the defendant voluntarily disclosed his location information to Google.

As an initial matter, the record makes clear that the consent flow language that the defendant agreed to is the consent flow language set forth in the McGriff affidavit. Gov't Ex. 3c at ¶ 7-8. McGriff swore that this language was used "across all applications and services, and across all Android devices and operating systems" on July 9, 2018, when the defendant opted in to Location History. Gov't Ex. 3c at ¶ 7. Moreover, every word of this language appears in the contemporaneous Norwegian report cited by the defendant, which states that its screen shots were taken in July and August of 2018. Gov't Ex. 3c at ¶ 7, 8; Def. Ex. 7 at 3-4. In contrast, the qz.com article comes from January 2018, and the Oracle report does not document when its screenshots were taken, but it has language similar to the qz.com article. Def. Ex. 7 at 1-2; Def. Ex. 11 at 4.

Thus, when the defendant argues based on language from the qz.com article, such as his repeated references to Google referring to Location History as creating a "private map," he is arguing based on opt-in language that Google did not present to the defendant during the opt-in process. Def. Post-Hr'g Suppl. Br. at 24, 32. Had defendant not encountered the supported consent

[4] The defendant claims that this process "boiled down to a single pop-up screen in Google Assistant," but his claim is not supported by the record. Def. Post-Hr'g Suppl. Br. at 24. The defendant's own expert conceded that he could not replicate the defendant's opt-in process. Suppression Hr'g Tr. 152. Only McGriff provided sworn testimony regarding all the steps of the opt-in process. Gov't Ex. 3 at at ¶ 10. Moreover, it is clear that the "single pop-up screen in Google Assistant" could not have done everything necessary for Google to store the defendant's Location History. For example, prior to that screen, the defendant would have had to sign into his Gmail account Okellochatrie55@gmail.com using his phone. The defendant may have used Google Assistant, but he still needed to complete all the steps described by McGriff in order for Google to store his Location History.

flow language, his attempt to opt in to Location History would have failed. Gov't Ex. 3c at ¶ 6. This Court should disregard arguments based on language from outside the supported consent flow presented to users on July 9, 2018.

The language from the supported consent flow of July 9, 2018, confirms that the defendant voluntarily disclosed his location to Google. Google informed the defendant that Location History "[s]aves where you go with your devices" and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com." Gov't Ex. 3c at ¶ 7. This language was concise, accurate, and easy to understand, and it set forth the core components of Google's Location History service: that Google would store the defendant's location information and that Google would use that information to provide services to the defendant. It also informed the defendant that he could see and delete his information through the Google website. *See id.* In addition, Google provided the defendant with the opportunity to obtain more detailed information concerning Location History by clicking an expansion arrow. Gov't Ex. 3c at ¶ 8. After Google presented this text to the defendant, he tapped "TURN ON." Gov't Ex. 3c at ¶ 10. This opt-in process establishes that the defendant voluntarily disclosed his location to Google.

The defendant makes numerous objections to this opt-in language, but his objections cannot obscure the fundamental fact that he agreed that Google would save his Location History and use it to provide him services. His objections therefore do not withstand scrutiny.

First, the defendant objects that "a user might reasonably infer that this 'private map' or saved data would be saved only on their device, not with Google." Def. Post-Hr'g Suppl. Br. at 25. Not only did Google not refer to a "private map," and not only is the storage location of data disclosed to Google to obtain Google services of no significance, but also Google's concise

consent-flow language made clear that the defendant's location data would be stored remotely: Google informed the defendant that he could review or delete his data "at account.google.com." Gov't Ex. 3c at ¶ 7. Google's use of this URL confirms that the data is stored remotely by Google, not on the user's device. In addition, via the expansion arrow, Google further informed potential Location History customers that "[t]o save this data, Google regularly **obtains location data from** your devices." Gov't Ex. 3c at ¶ 8 (emphasis added). Google informed the defendant that his data would be stored remotely.

Second, the defendant objects that Google did not inform users "about the frequency or sheer quantity of data collected." Def. Post-Hr'g Suppl. Br. at 26. The Supreme Court, however, has made clear that this objection lacks constitutional significance. In *Smith v. Maryland*, 442 U.S. at 745, the Court held that a phone company's choices regarding storage of dialed telephone number information did not "make any constitutional difference" because the defendant "voluntarily conveyed to it information that it had facilities for recording and that it was free to record." Here, the defendant similarly conveyed his location information to Google, and Google's decisions regarding how often to store that information lack constitutional significance. Moreover, Google did not mislead the defendant in any way. Google did exactly what the defendant agreed it should do: store where he went with his device. Because people often move fast and do not stay in one place for long, relatively frequent storage of location information by Google is necessary for it to provide quality service. Furthermore, Google informed the defendant that he could review his stored data at account.google.com. Thus, if he wanted to know more about how frequently Google stored his location, that information was available to him there.

Third, the defendant objects that "nothing explains that Location History will operate independently, regardless of whether the phone is in use." Def. Post-Hr'g Suppl. Br. at 26. Again,

this objection is based on a misinterpretation of Google's consent flow language. Google's concise explanation of its service stated that Location History "[s]aves where you go with your devices." Gov't Ex. 3c at ¶ 7. This categorical language includes no limitations or exceptions, thereby making clear that the Location History service did not depend on use of specific Apps. The defendant is essentially suggesting that Google should have added redundancy to Google's concise consent flow language, but redundancy was not required for the defendant to voluntarily disclose his location to Google. In addition, Google's expanded consent flow language stated that "[t]his data is saved even when you aren't using a specific Google service." Gov't Ex. 3c at ¶ 8.

Fourth, the defendant objects that "it would have been counterintuitive and difficult for Mr. Chatrie to disable and delete [his Location History], assuming he even knew about its existence." Def. Post-Hr'g Suppl. Br.at 27. But Google did not keep secret the data or the defendant's ability to delete it. It informed him: "You can see your data, delete it and change your settings at account.google.com." That language was more than sufficient to inform the defendant of his ability to delete information and where to find the details on how to do so. The defendant also seems to suggest that the distinction between deleting data and halting its future collection is hopelessly complicated, but nothing in that distinction is particularly confusing. On the contrary, given the defendant's ability to review his data at account.google.com, it would have been easy for him to confirm that he had, in fact, deleted his data.

In sum, the defendant's objections to Google's consent-flow language are premised on the notion that Google should have presented the defendant with a longer description of its service, rather than including the longer description through an optional expansion arrow. But Google's actual approach—concise text informing the defendant that it would save his location information and use it to provide him services, along with an expansion arrow linking to more detailed

information—is sufficient to establish that the defendant voluntarily disclosed his location information to Google. At the evidentiary hearing, McGriff explained the practical result of the defendant's approach: a "wall of text" that users would not be inclined to read. Suppression Hr'g Tr. 441.[5]

*c. Google's Privacy Policy*

Finally, Google's Privacy Policy further supports the fact that the defendant voluntarily disclosed his location information to Google. Courts rely on terms of service and privacy policies in evaluating whether a service provider's disclosure of information to the government violates the Fourth Amendment. *See, e.g.*, *United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019) (holding that that T-Mobile's disclosure of cell-site information to the government did not violate Adkinson's Fourth Amendment rights because Adkinson "agreed to T-Mobile's policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests,

[5] The defendant points to criticism of Google's Location History service from other parties, *see* Def. Post-Hr'g Suppl. Br. at 29-30, but this Court should give such criticism no weight. First, this Court did not admit that criticism for the truth of the matter asserted. Second, the record in this case sets forth the actual consent flow language Google presented to the defendant. Thus, there is no need for this Court to defer to the views of various third parties about Google's opt-in procedures—views potentially based on different language than that actually presented to the defendant. In addition, those critics are not attempting to address the question before this Court: whether, for Fourth Amendment purposes, the defendant voluntarily conveyed his location information to Google.

property, or safety").[6] Here, through Google's Terms of Service, the defendant agreed that Google could use his information in accordance with its Privacy Policy. Suppression Hr'g Tr. 382; Gov't Ex. 5a at 3. And that Privacy Policy stated: "We collect information about your location when you use our services, which helps us offer features like driving directions for your weekend getaway or showtimes for movies playing near you." Gov't Ex. 5 at 4. In addition, the Privacy Policy contained specific examples pertaining to Location History, including: "you can turn on Location History if you want traffic predictions for your daily commute." *Id.* at 9. This language confirms that the defendant agreed to share his location with Google in order for Google to provide him with location-based services. Furthermore, the Privacy Policy provided an additional explanation to the defendant of his ability to delete his information. *Id.* at 11-12.

3. The defendant has no reasonable expectation of privacy in two hours of Google location information under the reasoning of *Carpenter*.

In *United States v. Carpenter*, 138 S. Ct. 2206, 2217 & n.3 (2018), the Supreme Court determined that individuals have a "reasonable expectation of privacy in the whole of their physical movements," and it held "that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search." The Court emphasized that its decision was "a narrow one," and it explicitly declined to determine whether there is a "limited period" for which the government can

[6] The defendant fundamentally misreads *Smith v. Maryland* when he claims that it supports his argument that courts should not consider a company's Privacy Policy in evaluating whether a customer has a reasonable expectation of privacy. *See* Def. Post-Hr'g Suppl. Br. at 27. In fact, *Smith*'s determination that users have no reasonable expectation of privacy in dialed phone numbers was based in part on Privacy Policy-like statements included in phonebooks. *See Smith*, 442 U.S. at 742-43 ("Most phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'"). In contrast, *Smith* found no Fourth Amendment significance in the phone company's interal data storage practices and definition of local-dialing zones, which do not at all resemble privacy policies. *See id.* at 745.

acquire cell phone location information without implicating the Fourth Amendment, or whether a cell tower dump constituted a search. *Id.* at 2217 n.3, 2220.

Although *Carpenter* declined to resolve whether obtaining two hours of cell phone location information constitutes a search, *Carpenter*'s reasoning suggests it does not, because *Carpenter* is focused on protecting a privacy interest in long-term, comprehensive location information. The Court began its opinion by framing the question before it as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Carpenter*, 138 S. Ct. at 2212. The Court emphasized that long-term cell-site information created a "comprehensive record of the person's movements" that was "detailed" and "encyclopedic." *Id.* at 2216–17. It explained that "this case is not about 'using a phone' or a person's movement at a particular time." Rather, the Court explained, the case concerned "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220. By this standard, the government did not conduct a search when it obtained the two hours of the defendant's location information pursuant to the geofence warrant. Rather than providing an encyclopedic chronicle of the defendant's life, the information disclosed by Google provided a summary of his location for less than half an afternoon. This information is not quantitatively or qualitatively different from information that could be obtained from other sources, such as surveillance video or live witnesses.

In addition, in numerous cases involving other sophisticated new technologies, lower courts held that *Carpenter* protects only comprehensive, long-term location information. For example, the Seventh Circuit recently held that real-time tracking of a specified cell phone over a period of approximately six hours was not a search. *See United States v. Hammond,* — F.3d —, 2021 WL 1608789, at *7-*11 (7th Cir. Apr. 26, 2021). The Seventh Circuit previously determined

that a cell tower dump was not a search, and two other district courts reached the same result. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (stating that *Carpenter* "did not invalidate warrantless tower dumps (which identified phones near *one location* (the victim stores) at *one time* (during the robberies))" (emphasis in original)); *United States v. Walker*, 2020 WL 4065980, at *8 (W.D.N.C. July 20, 2020) (concluding that the "privacy concerns underpinning the court's holding in *Carpenter* do not come into play" for a cell tower dump, which is limited to "particular *place* at *a limited time*") (emphasis in original)); *United State v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021) (stating that *Carpenter* "centrally relied on the strong Fourth Amendment privacy interests implicated when law enforcement monitors or obtain voluminous, detailed cell phone information of a person's physical presence compiled over a lengthy period that effectively delineates the contours of the individual's life and communications").[7] These cases all support the conclusion that the United States did not infringe the defendant's Fourth Amendment interests when it obtained two hours of his location information from Google.

Significantly, *Carpenter* did not reject the third-party doctrine or "disturb the application

[7] Similarly, courts have rejected a broad interpretation of *Carpenter* in cases involving automatic license plate reader databases, which record the time and place a license plate is observed. Obtaining a large amount of location information about an individual from such a database could potentially implicate *Carpenter*'s concerns regarding comprehensive location information. But investigators do not conduct a search when they obtain only a small quantity of location information from such a database. *See Commonwealth v. McCarthy*, 484 Mass. 493, 494 (2020) ("[W]hile the defendant has a constitutionally protected expectation of privacy in the whole of his public movements, an interest which potentially could be implicated by the widespread use of [automatic license plate readers], that interest is not invaded by the limited extent and use of ALPR data in this case."); *United States v. Yang*, 958 F.3d 851, 862 (9th Cir. 2020) (Bea, J., concurring) (stating that a query of a large automatic license plate recognition database that revealed only a single location point for Yang was not a search under Carpenter because "the information in the database did not reveal 'the whole of [Yang's] physical movements.'").

of *Smith* and *Miller*." *Carpenter*, 138 S. Ct. at 2220. Instead, *Carpenter* held that cell phone users do not voluntarily disclose their cell-site records to the phone company because cell-site information is collected "without any affirmative act on the part of the user beyond powering up," because "there is no way to avoid leaving behind a trail of location data," and because carrying a cell phone "is indispensable to participation in modern society." *Carpenter*, 138 S. Ct. at 2220. These factors are not present here. Google could not obtain and store the defendant's location without his undertaking multiple affirmative acts, including signing in to Google on his phone, enabling the phone's device location setting, enabling location reporting, and opting in to Location History. Gov't Ex. 3 at ¶ 10. The defendant also had discretion to delete any or all of his Location History. Gov't Ex. 3 at ¶ 15; Suppression Hr'g Tr. 321, 388, 416. And none of the services associated with Google's storage of Location History are indispensable to participation in modern society. In fact, approximately two-thirds of Google's users reject those services. Gov't Ex. 3 at ¶ 13; Suppression Hr'g Tr. 387.

Citing *Carpenter*, the defendant asserts that this Court should disregard the third-party doctrine, "Even If Mr. Chatrie Intentionally Enabled Location History." Def. Post-Hr'g Suppl. Br at 31. To do so, however, would disregard controlling precedent. *Carpenter* held based on facts specific to the cell phone provider context that Carpenter had not voluntarily disclosed his cell phone location information to the phone company, but it did not otherwise reverse or limit the third party doctrine. *See Carpenter*, 138 S. Ct. at 2220. Thus, if this Court determines that the defendant intentionally disclosed his location to Google, this Court must conclude that the defendant had no reasonable expectation of privacy in the location information the United States obtained from Google, as "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. at 743-44.

4. The defendant's remaining arguments are without merit.

None of the defendant's remaining arguments establish that the United States infringed the defendant's Fourth Amendment interess when it obtain location information from Google.

First, he argues that "Location History Is At Least As Precise as CSLI," but he fails to explain why that fact creates a reasonable expectation of privacy. Def. Post-Hr'g Suppl. Br. at 20. The third-party doctrine applies to information voluntarily disclosed to a third party; it includes no exception for accurate location information. And the Supreme Court in *Carpenter* assumed that cell-site information "is rapidly approaching GPS-level precision," *Carpenter*, 138 S. Ct. at 2219, but *Carpenter* still only protected disclosure of long-term, comprehensive location information.

Second, the defendant claims that "A Search of Location History Data Is Highly Intrusive," but this argument is neither supported by facts in the record nor sufficient to establish that he had a reasonable expectation of privacy in his location information. Def. Post-Hr'g Suppl. Br. at 21-23. As an initial matter, the principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" is not limited to information which is not particularly revealing about an individual. Conversations with others, dialed telephone numbers, and bank records can all contain sensitive information that an individual would like to keep private, but they are all subject to the third-party doctrine. Furthermore, the information the United States obtained from Google in this case was not particularly sensitive. Indeed, the defendant makes no claim that it revealed anything sensitive about him at all. Neither presence at a bank nor movements along public roads are particularly sensitive information. *See, e.g.*, *United States v. Knotts,* 460 U.S. 276, 285 (1983) (holding that monitoring movements along public roads using a

transponder installed in a container of chemicals was not a search).[8]

Third, the defendant cites the fact the United States obtained information about other Google users, but he provides no explanation of how this fact supports his claim that he had a reasonable expectation of privacy in the location information disclosed by Google. Def. Post-Hr'g Suppl. Br. at 22. In addition, his attempt to rely on the Fourth Amendment interests of others is foreclosed by Supreme Court precedent. The Supreme Court has squarely held that Fourth Amendment rights "may not be vicariously asserted." *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Defendants lack standing to challenge the government obtaining others' cell phone location information. *See, e.g.*, *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016).

Fourth, the defendant cites the fact that Google filtered through its entire Location History database to find information responsive to the warrant, Def. Post-Hr'g Suppl. Br. at 22, but he fails to explain how this filtering would give him an expectation of privacy. In determining whether a defendant has a reasonable expectation of privacy, courts consider the totality of the circumstances regarding the relationship between the defendant and the object of the search, *see United States v. Castellanos*, 716 F.3d 828, 846 (4th Cir. 2013), but they do not consider the particular legal process used by the government to obtain that object. The defendant would have had no reasonable expectation of privacy in two hours of his Google Location History regardless of whether the United States obtained it using a geofence warrant or a warrant explicitly identifying his account.

[8] The defendant's claim that "the defense was easily able to determine the likely identities of at least three individuals" from the geofence location information is not supported by the record. *See* Def. Post-Hr'g Suppl. Br. at 22. The defense's expert witness stated that he had not "figured out who anyone is." Suppression Hr'g Tr. 151. Moreover, neither identifying someone present at a bank nor identifying the neighborhood that someone visits (or even their home) is particularly invasive.

Fifth, the defendant is mistaken when he argues that "[u]nder the government's theory, people do not have an expectation of privacy in any data stored with a third-party or service provider, other than long-term CSLI." Def. Post-Hr'g Suppl. Br. at 31. Here, the defendant has no reasonable expectation of privacy in his location information because he disclosed it to Google in order for Google to provide him with location-based services. This principle does not apply in many common circumstances involving online service providers. For example, when an email service provider transmits and stores email on behalf of a customer, the email service does not typically depend on the substantive contents of the email, so the user may retain a reasonable expectation of privacy in email content information.

Finally, the defendant adopts by reference his "property-based arguments," Def. Post-Hr'g Suppl. Br. at 32, but his argument remains contrary to the fundamental principle that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443. The defendant cites no case—and the United States is aware of no case—in which a court has relied on a "property-based theory" to discard the third-party doctrine of *Smith* and *Miller* or prevent witnesses from providing evidence to the government. Justice Gorsuch's solo dissent in *Carpenter* did contemplate abandoning the third-party doctrine based on some sort of property rights theory of the Fourth Amendment, *see Carpenter*, 138 S. Ct. at 2262-72 (Gorsuch, J., dissenting), but a solo dissent is not the law, and the third-party doctrine of *Smith* and *Miller* remains binding law.

B. *The Geofence Warrant Satisfied the Fourth Amendment*

The geofence warrant did not remotely resemble a general warrant. As set forth below, the warrant satisfied the Fourth Amendment because it was supported by probable cause and specified its object with particularity.

More generally, the facts of this case illustrate why use of a geofence warrant involves no unreasonable search or seizure. When law enforcement officers sought the warrant, they were investigating a serious violent crime, and they had reason to believe that the perpetrator posed a danger to the public if not identified and apprehended. Suppression Hr'g Tr. 622. The geofence warrant enabled them to solve the crime and protect the public by allowing them to obtain a limited and focused set of records from Google: location information over a two-hour interval of three identified and six unidentified individuals, and limited location information over a one-hour interval of ten other unidentified individuals.

The defendant argues that investigators should have taken a different path: "track down the owner of the car the suspect was seen in and compare that information to cell phone numbers that had connected with a nearby cell phone tower." Def. Post-Hr'g Suppl. Br. at 42. This approach would have required investigators to obtain a cell tower dump covering a much broader area, which likely would have revealed location information about thousands of people. Suppression Hr'g Tr. 55. It would have required them to obtain a list of everyone who had a blue Buick. Suppression Hr'g Tr. 578. And then it would have required them to further investigate everyone who fell within the overlap of these sets.

Although the defendant's approach would also have complied with the Fourth Amendment, it would have been substantially more intrusive than the geofence warrant, as well as being less likely to succeed and more expensive. It would be a very strange result if the Fourth Amendment were to bar use of a precise, focused investigative technique like a geofence warrant, and if it instead forced investigators to cast much broader nets. Fortunately, the defendant is mistaken, and the geofence warrant complied with the Fourth Amendment.

1. The Geofence Affidavit Established Probable Cause

Probable cause requires only "a fair probability, and not a prima facie showing, that contraband or evidence of a crime will be found in a particular place." *United States v. Bosyk*, 933 F.3d 319, 325 (4th Cir. 2019) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotation marks omitted)). It is "not a high bar." *Id.* (quoting *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018)). In addition, this Court does not conduct *de novo* review concerning the existence of probable cause: "the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004) (quoting *Gates*, 462 U.S. at 238–39).

Here, the affidavit in support of the geofence warrant established an ample basis for the issuing magistrate's finding of probable cause. In particular, the affidavit established: (1) that an unknown subject committed an armed bank robbery at a particular place and time; (2) that prior to the robbery, the robber held a cell phone to his ear and appeared to be speaking with someone; (3) that the majority of cell phones were smartphones; (4) that "[n]early every" Android phone "has an associated Google account," and that Google "collects and retains location data" from such devices when the account owner enables Google location services; and (5) that Google can collect location information from non-Android smartphones if the devices are "registered to a Google account and the user has location services enabled." Gov't Ex. 2 at 6-7. From this information, there was a substantial basis for the magistrate to conclude that there was a fair probability that Google possessed evidence related to the robbery.

One United States Magistrate Judge recently explained his basis for issuing a geofence warrant in an arson investigation, including his determination that the warrant was supported by probable cause. *See In re Search Warrant Application*, 497 F. Supp. 3d 345 (N.D. Ill. 2020)

(hereinafter, "Harjani Opinion"). In that investigation, there was "no evidence in the affidavit that any of the suspects possessed cell phones." *Id.* at 355. Nevertheless, the magistrate judge noted that judges "may draw reasonable inferences about where evidence is likely to be found based on the nature of the evidence and the offense," and he determined that it was reasonable to infer that suspects and passerby witnesses would have cell phones, and that Google would have information about their location and identity. *See id.* at 355-56. He concluded that "the affidavit, when considering the totality of the circumstances and the agent's training and experience, allows the Court to conclude there is a fair probability that location data at Google will contain evidence of the arson crime, namely the identities of perpetrators and witnesses to the crime." *Id*. Here, where the robber used his phone just before the robbery, the basis for the magistrate's finding of probable cause was stronger than in the investigation addressed in the Harjani Opinion.

The probable cause determination for a geofence warrant is similar to that for a tower dump warrant, and in *United States v. James*, No. 18-cr-216, 2019 WL 325231 (D. Minn. Jan. 25, 2019), the district court held that a series of tower dump warrants satisfied the Fourth Amendment. In *James*, the government used tower dump warrants to solve a series of robberies. The defendant there argued that there was no probable cause for the warrants because it was "unknown whether a phone was used by the suspect before or after the robbery." *Id.* at *3. Nevertheless, the district court found that probable cause existed based on the affiant's representations about the "ubiquitous nature" of cell phones, the likelihood of criminals using cell phones, and the storage by cell phone companies of location information. *Id.* This reasoning similarly supports the magistrate's finding of probable cause for the geofence warrant in this case.

Two other magistrate judges from the Northern District of Illinois have written opinions denying applications for geofence warrants. The first magistrate judge found that the bounds of

the geofence sought by the government were too broad, but he stated that the government "could easily have sought a constitutionally valid search warrant" if it had "constrained the geographic size of the geofence and limited the cellular telephone numbers for which agents could seek additional information to those numbers that appear in all three defined geofences." *See In re Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *7 (N.D. Ill. July 8, 2020). Whether the bounds of a particular geofence are too broad will always be based on the facts and circumstances of the investigation. In this investigation, the bounds of the geofence were appropriately drawn for the magistrate to conclude that there was a fair probability that Google possessed the specified evidence of crime. *See* Suppression Hr'g Tr. 523 (discussing the bounds of the geofence).

The second magistrate judge held that probable cause for a geofence warrant was lacking because there was not "probable cause to believe *every* person who entered the location engaged in the criminal activity." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 752 (N.D. Ill. 2020) (emphasis in original). As the Harajani Opinoin recognized, however, "it is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are impacted." Harjani Opinion, 497 F. Supp. 3d at 361-62. For example, the Fourth Amendment does not bar a search warrant to search a residence that a suspect shares with others. Both the defendant here and the second magistrate judge base their arguments on *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), in which the Supreme Court held that the probable cause that supported a warrant to search a tavern and its bartender for drugs did not extend to a search of tavern patrons. But *Ybarra* is not a general limitation on search warrants that might reveal information concerning non-suspects; it merely held that the probable cause to search a commercial premises for drugs did not extend to a search of the businesss's patrons. The Harjani

Opinion explains why *Ybarra* does not limit a geofence warrant like the one here: "the government has established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence, and the request is sufficiently particular to avoid any concerns resulting from *Ybarra*." Harjani Opinion, 497 F. Supp. 3d at 362 n.6.

The defendant makes several arguments that attempt to narrow or redefine the meaning of "probable cause." These arguments lack merit, and this Court should reject them.

First, the defendant argues that the geofence warrant lacked probable cause "because investigators admittedly had no suspects." Def. Post-Hr'g Suppl. Br. at 33. However, a search warrant need not identify specific suspects—all it must do is establish a fair probability that specified evidence will be found in the place to be searched. For example, in *Zurcher v. Stanford Daily*, 436 U.S. 547, 551 (1978), the Supreme Court approved a search warrant that authorized seizure from a newspaper of photographs of unidentified individuals who had assaulted police officers. The defendant cites no case suggesting that a warrant cannot be used to solve crime.

Second, the defendant asserts that "[p]robable cause must be based on individualized facts, not group probabilities," and he claims it was improper to infer that "the robber was a Google user or had Location History enabled." Def. Post-Hr'g Suppl. Br. at 33-34. This is error: a magistrate may "draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant." *Illinois v. Gates*, 462 U.S. 213, 240 (1983). Here, the magistrate's finding of probable cause was based on a combination of specific facts (that the bank had been robbed and that the robber carried a cell phone) and reasonable inferences (that there was a fair probability that Google stored location evidence pertaining to this crime). Warrants commonly rely on a combination of specific facts and reasonable inferences, and the defendant cites no contrary case

law. For example, in *United States v. Jones*, 942 F.3d 634, 639-40 (4th Cir. 2019), the Fourth Circuit held that a magistrate had made a reasonable inference that evidence of a defendant's threats would be found at his home. Here, the magistrate similarly made a reasonable inference that Google stored evidence of the robbery.

Third, the defendant's argument is based on an improperly constricted view of what would constitute evidence of the robbery. He focuses on whether "the robber was a Google user," Def. Post-Hr'g Suppl. Br. at 33, but the issuing magistrate here had additional reasons to believe that location information held by Google would be evidence. Investigators could use the location information directly to reconstruct what took place at the crime scene at the time of the crime. They could use it to identify any accomplices. They could use it to identify potential witnesses and obtain further evidence. They could use it to corroborate and explain other evidence, including surveillance video. They could use it to rebut potential defenses raised by the robber, including an attempt by the robber to blame someone else for his crime. Thus, although the affidavit did in fact establish a fair probability that Google would have evidence concerning the robber, the probable cause established by the warrant extended well beyond that, and it was reasonable for the magistrate to conclude that all of the information that fell within the scope of the warrant constituted evidence of crime.[9]

[9] *Messerschmidt v. Millender*, 565 U.S. 535 (2012), supports this understanding of what may constitute evidence for purposes of a search warrant. In *Messerschmidt*, police obtained a warrant for "all guns and gang-related material" in connection with a known gang member shooting at his ex-girlfriend. *Id.* at 539. In a civil suit under 42 U.S.C. § 1983, Millender challenged the warrant as overbroad, but the Supreme Court rejected the suit based on qualified immunity. *See id.* The Court provided multiple reasons why it was not unreasonable for a warrant to seek "all gang-related materials" in connection with someone shooting at his ex-girlfriend. These reasons included that it could "help to establish motive," that it could be "helpful in impeaching [the shooter]," that it could be helpful in "rebutting various defenses," and that it could "demonstrat[e] [the shooter's] connection to other evidence." *Id.* at 551-52.

2. The Geofence Warrant Was Not Overbroad and Specified its Objects with Particularity

Under the Fourth Amendment, "a valid warrant must particularly describe the place to be searched, and the persons or things to be seized." *United States v. Kimble*, 855 F.3d 604, 610 (4th Cir. 2017) (internal quotation marks omitted). In addition, the items specified to be seized pursuant to a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). The test "is a pragmatic one" that "may necessarily vary according to the circumstances and type of items involved." *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979) (quoting *United States v. Davis*, 542 F.2d 743, 745 (8th Cir. 1976)). Here, the geofence warrant satisfied these requirements.

*a. Overbreadth*

The geofence warrant was not overbroad because it was narrowly constrained based on location, dates, and times. The warrant sought only location and identity information from Google regarding a two-hour interval for individuals present at the site of a robbery during a one-hour window. Based on the facts and circumstances investigators knew about the robbery, it was appropriately tailored toward its investigatory purpose, which was to obtain evidence to help identify and convict the armed bank robber. The geofence was based on specific features of the site of the robbery. For example, it went up to but did not cover Price Club Boulevard to the east, and it covered the area where the robber had parked. Suppression Hr'g Tr. 523. Like the geofence warrant approved in the Harjani Opinion, the government "established a fair probability that location data obtained will retrieve location data of perpetrators, co-conspirators and witnesses within the geofence." Harjani Opinion, 497 F. Supp. 3d at 362 n.6. Because the evidence the

government was authorized to obtain was "no broader than the probable cause on which it is based," the warrant was not overbroad.

The cell tower dump opinion *James* provides additional authority that the warrant here was not overbroad. In *James*, the defendant challenged the tower dump warrants used to identify him as a robber because they "allowed law enforcement to identify the location of hundreds if not thousands of cell phone users on specific days during specific time frames." *James*, 2019 WL 325231 at *3. The district court, however, found that the warrants satisfied the Fourth Amendment because they sought information that was "constrained—both geographically and temporally—to the robberies under investigation." *Id.* This reasoning is fully applicable here: the geofence warrant was appropriately constrained in space and time to obtain evidence of the robbery. Indeed, the location information obtained from Google was more narrowly constrained than the location information in James. The 150-meter radius of the geofence warrant is smaller than most cellular sites, and the government only obtained location information regarding 19 individuals, most of them never identified, rather than hundreds or thousands.[10]

The defendant argues that the geofence warrant was overbroad because Google filtered its Location History database to comply with it, but this argument is without merit. Def. Post-Hr'g Suppl. Br. at 33. He cites no case law holding that a service provider may not review a large data set in order to produce a narrowly defined set of information. Such process is not new: for example, in response to a subpoena, a phone company may review every call made by all its customers in order to find calls made to a specified phone number. *See Ameritech Corp. v.*

[10] The defendant argues that cell tower dumps are more limited than geofence warrants because cell phone companies "'index' data based on location." Def. Post-Hr'g Suppl. Br. at 35. But as discussed further below, a company's internal data structures have no Fourth Amendment significance. *See infra* pp. 36-37.

*McCann*, 403 F.3d 908, 910 (7th Cir. 2005).

Here, Google stores its users' location information in a single database, Sensorvault. Gov't Ex. 3 at ¶ 11. Google acesses it users' location information freely to provide them and others with location-based services. For example, Google offers its advertisers a service called "radius targeting," which requires Google to determine whether a customer is within a specified distance of a specified point. Suppression Hr'g Tr. 198. And then Google further accesses users' location information to measure store visit conversions, which it shares with the advertisers. Gov't Ex. 3 at ¶ 14; Suppression Hr'g Tr. 196-97. Here, the warrant mandated an equivalent to radius targeting, but for the purpose of solving a bank robbery, rather than selling a product. The Fourth Amendment does not prohibit Google, in response to warrant, filtering data that it accesses and uses for its own business purposes.

Moreover, Google's review of a large set of data to comply with the geofence warrant is a result of Google's internal data storage practices, not an overbroad warrant. It would be possible for Google to create an additional Location History database indexed by location. Suppression Hr'g Tr. 402-03. This database would enable Google to comply with a geofence warrant—and produce the exact same data as Google currently produces—without filtering the data of all customers. The constitutionality of a search warrant does not depend on a service provider's internal data storage practices invisible to customers and the government alike. For example, in *Smith v. Maryland*, the Supreme Court held that a phone company's internal practices regarding storage of dialed number information did not "make any constitutional difference." *Smith*, 442 U.S. at 745. This reasoning is fully applicable here to Google's choice of internal data structures. The appropriate measure for the breadth of the geofence warrant here is the data sought by the warrant, which resulted in the government obtaining location information for only 19 individuals,

all of whom were near the bank at the time of the robbery.

*b. Particularity*

The geofence warrant specified the items to be seized with unusual precision. The warrant authorized disclosure from Google of two hours of location information associated with electronic devices that were, within a 30 minutes on either side of a bank robbery, within 150 meters of a specified point, as well as specified subscriber information associated with those devices. Gov't Ex. 2 at 4-5. Most warrants require a human to make judgments regarding whether particular items fall within the scope of the items to be seized, but here, Google could use a computer algorithm to find the responsive information. The defendant's assertion that "[t]he items to be seized are not specified" by the geofence warrant is therefore wrong. Def. Post-Hr'g Suppl. Br. at 37.

The defendant asserts that the warrant left too much discretion to Google, but the warrant left Google no discretion at all. *See* Def. Post-Hr'g Suppl. Br. at 38. First, the defendant complains that "Google decided to search Location History data, as opposed to Web & App Activity or Google Location Services data," *see id.*, but only the Location History database held information responsive to the warrant. Gov't Ex. 3 at ¶ 20; Suppression Hr'g Tr. 211. Second, the defendant complains that Google "picked a method of calculating which devices were inside the geofence that generated a high number of false positives," Def. Post-Hr'g Suppl. Br. at 38, but the warrant itself directed Google to disclose information for devices "inside the described geographical area" during the time of the robbery. Gov't Ex. 2 at 4. Google correctly interpreted this language to mean that Google should disclose information concerning devices whose latitude and longitude coordinates fell within the circle specified by the warrant. Although there always remains a possibility of imprecision in Google's location information, and a defendant may certainly challenge at trial the weight given to this information, that possibility does not make a warrant

insufficiently particular.[11]

Nor was there anything improper about FBI TFO Hylton's correspondence with Google, in which he ultimately requested that Google produce step 2 location information about nine individuals. Suppression Hr'g Tr. 622, 642; Gov't Ex. 4 at 9. Google remains an independent actor, and courts have held that a provider like Google has a due process right to object to an order directing it to comply with a search warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1157 (3d Cir. 1979). Where a service provider produces a portion of the information specified by legal process, the United States does not violate the Fourth Amendment when it chooses not to litigate over the rest. A contrary rule would waste judicial resources and harm privacy. Nothing in the execution of the geofence warrant supports the defendant's argument that the warrant was insufficiently particular.

The defendant also challenges the warrant because it included the second and third steps of its three-step process, thereby allowing investigators to obtain less than the maximum quantity of location and identity information that the warrant authorized. *See* Def. Post-Hr'g Suppl. Br. at 38-39. The warrant, however, established probable cause for all the evidence that law enforcement could have obtained: identity information and two hours of location data for all individuals present

[11] The defendant exaggerates the magnitude of uncertainty associated with Google's location information. He emphasizes individual location measurements that had a large display radius. These measurements, however, were in general accompanied by other measurements for the same device with smaller display radius. For example, the defendant points to one measurment in the initial production from Google with a display radius of 387 meters. *See* Def. Post-Hr'g Suppl. Br. at 17. However, a separate measurement point for that same device taken only 23 seconds before had a display radius of only 84 meters. *See* FBI CAST Report at 22 (noting initial GeoFence returns, including for Device ID 702354289); Def. Ex. 3 (cell entries 208 and 209 for Device ID 702354289). As Special Agent D'Errico explained, Google location data of this nature (two records close in time with the same center point, but a larger second display radius) indicates that the device is traveling. Suppression Hr'g Tr. 532. The uncertainty associated with the second point does not affect the accuracy of the first.

at the site of the robbery during the hour of the robbery. The information specified by a warrant must be "no broader than the probable cause on which it is based," *Hurwitz*, 459 F.3d at 473, but officers do not violate the Fourth Amendment if they ultimately seize less evidence than the maximum a warrant authorizes. The Harjani Opinion approved a multiple-step geofence warrant for precisely this reason: "[T]he government has established probable cause to seize all location and subscriber data within the geofence locations identified. Whether it chooses to obtain all that information, or partial information, is of no matter to the Court's consideration of the constitutionality of the warrant under the Fourth Amendment." Harjani Opinion, 497 F. Supp. 3d at 362.

The most heavily-litigated search warrant in history—the search warrant in the investigation of the Playpen child pornography website—included a similar component that allowed investigators to prioritize the evidence they seized, and courts have agreed that that component did not violate the Fourth Amendment.[12] Playpen was a dark web child pornography site with over 158,000 members. *See United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018). FBI investigators obtained a warrant authorizing a search of the computers of everyone who logged into Playpen for 30 days. *See id.* at 689. The attached affidavit, however, allowed the FBI to choose to obtain less than the maximum amount of information the warrant authorized. It explained that that "in executing the requested warrant, the FBI may deploy the NIT more

[12] Eleven Courts of Appeals have considered various challenges to the Playpen warrant, and all have ultimately rejected suppression. *See United States v. Taylor*, 935 F.3d 1279, 1281 (11th Cir. 2019) ("[W]e become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed."). Approximately 100 district court cases have resolved suppression motions challenging the Playpen warrant. As discussed in Section C below, the Fourth Circuit rejected a challenge to the particularity of the Playpen warrant based on the good-faith exception. *See United States v. McLamb*, 880 F.3d 685, 689-91 (4th Cir. 2018).

discretely against particular users." *United States v. Anzalone*, 208 F. Supp. 3d 358, 363 (D. Mass. 2016).

Some defendants argued that the discretion given the FBI in executing the Playpen warrant violated the Fourth Amendment's particularity requirement, but courts uniformly rejected this argument. For example, in *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016), the court concluded that "the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site." *See also Anzalone*, 208 F. Supp. 3d at 368 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Similarly, the fact that investigators here could have and did narrow the information obtained from Google is immaterial, as the geofence warrant was based on probable cause and appropriately authorized seizure of location and identity information of anyone at the site of the robbery. Rather than violating the Fourth Amendment, the three-step process allowed investigators to further protect privacy.

Finally, even if there were a particularity problem in the three-step process for the geofence warrant, the appropriate remedy would at most be to sever the second step of the warrant and to suppress second-step information. "[E]very federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible." *United States v. Sells*, 463 F.3d 1148, 1154–55 (10th Cir. 2006); *see also United States v. Jones*, 2018 WL 935396, at *16–*18 (E.D. Va. Feb. 16, 2018) (discussing and applying doctrine of severance).

Here, the first step of the geofence warrant targeted narrow and clearly-defined information: anonymized location information for devices within 150 meters of the bank during

the hour of the robbery. Even if this Court were to find the second step to be constitutionally inadequate, the appropriate remedy would thus be to sever the second step and retain the first. In addition, first-step information alone was sufficient for investigators to recognize that the defendant's account likely belonged to the robber. Suppression Hr'g Tr. 549-50. Thus, even if this Court were to sever the warrant and suppress second-step information from Google, the subsequent investigation of the defendant would not be the fruit of the poisonous tree.[13]

C. *Evidence from the Geofence Warrant Should Not Be Suppressed Because Investigators Relied on it in Good Faith*

Even assuming the geofence warrant was lacking in probable cause or particularity, suppression would not be an appropriate remedy. Suppression is a remedy of "last resort," to be used for the "sole purpose" of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression "outweigh its heavy costs." *Davis v. United States*, 564 U.S. 229, 236-37 (2011). "The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144.

Search warrants for Google information about the location of its users are a new investigative technique, and there were no judicial opinions analyzing them under the Fourth Amendment when FBI TFO Hylton sought his warrant. In *United States v. McLamb*, 880 F.3d

[13] Under *Bynum*, 604 F.3d at 164, the defendant lacks a reasonable expectation of privacy in subscriber information obtained under step three of the geofence warrant, and he therefore lacks standing to challenge that portion of the warrant.

685 (4th Cir. 2018), the Fourth Circuit rejected suppression in this circumstance. The court held that when considering a motion to suppress the fruits of a novel investigative technique, suppression was inappropriate where the investigating officer consulted with counsel and then sought a warrant:

> But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what Leon's 'good faith' expects of law enforcement. We are disinclined to conclude that a warrant is 'facially deficient' where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

*McLamb*, 880 F.3d at 691. Here, Detective Hylton followed the approach endorsed by *McLamb*. He had consulted with prosecutors before seeking both state and federal geofence warrants. Suppression Hr'g Tr. 603-04. He had previously obtained geofence warrants from both state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. No prosecutor or judge had ever found a problem with these warrants. Suppression Hr'g Tr. 604-05. In this investigation, he then sought and obtained a search warrant from a state magistrate. Detective Hylton thus did what *McLamb* calls for, and the good-faith exception precludes suppression here.

The defendant also insinuates that investigators did something wrong by using a go-by from the Computer Crime and Intellectual Property Section at the Department of Justice. Def. Post-Hr'g Suppl. Br. at 3-4. But *McLamb* affirmatively encourages such consultation: it applied the good faith exception where investigators had consulted with experts from another Department of Justice section, the Child Exploitation and Obscenity Section. *See McLamb*, 880 F.3d at 691.

The defendant notes that FBI TFO Hylton had received no training on geofence warrants, Def. Post-Hr'g Suppl. Br. at 44, but there is no indication in *McLamb* that the agents there had received training on darknet child pornography warrants. Indeed, such trainings may not exist

when a new investigative technique first arises. *McLamb* calls for direct consultation with prosecutors and then seeking a warrant, not meeting a bureaucratic training requirement. Consulting directly with experts is an effective form of training, even if it is not officially categorized as such.

Alternatively, suppression is inappropriate under the traditional good-faith analysis of *United States v. Leon*, 468 U.S. 897 (1984). When police act in "objectively reasonable reliance on a subsequently invalidated search warrant" obtained from a neutral magistrate, "the marginal or nonexistent benefits produced by suppressing evidence … cannot justify the substantial costs of exclusion." *Id.* at 922. *Leon* identified four circumstances in which an officer's reliance on a warrant would not be objectively reasonable:

> (1) when the issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) when "the issuing magistrate wholly abandoned his judicial role …"; (3) when "an affidavit [is] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) when "a warrant [is] so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

*United States v. Perez*, 393 F.3d 457, 461 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923). None of these circumstances are present in this case.

The defendant argues that the good faith exception does not apply here because the affidavit was so lacking in indicia of probable cause that reliance on it was unreasonable, *see* Def. Post-Hr'g Suppl. Br. at 42-43, but he is mistaken. As an initial matter, "the threshold for establishing this exception is a high one" because "[o]fficers executing warrants are not often expected to question the conclusions of an issuing authority." *United States v. Seerden*, 916 F.3d 360, 367 (4th Cir. 2019) (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012)). The defendant claims that the warrant was based on "conjecture," Def. Post-Hr'g Suppl. Br. at 42-43, but in fact

it was based on facts and reasonable inferences from those facts. The affidavit established that the bank robber had a cell phone, that most cell phones are smartphones, and that nearly every Android phone user and some non-Android phone users use Google, and that Google may store user location information. Based on these facts, the executing officers' belief that the warrant to Google was issued based on probable cause was not entirely unreasonable, and the good-faith exception thus precludes suppression.

The defendant also argues that the good faith exception does not apply because the warrant was so facially deficient in failing to specify the things to be seized that officers could not reasonably rely on it. *See* Def. Post-Hr'g Suppl. Br. at 43. But as discussed previously, the warrant was unusually specific: Google determined the responsive information using a computer algorithm. As discussed above at pages 37-38, the warrant was limited to location information over a two-hour interval, as well as accompanying identity information, for individuals present at the site of the robbery during a one-hour interval.

The defendant further argues that the warrant left too much discretion to Google, Def. Post-Hr'g Suppl. Br. at 44, but the warrant left no discretion to Google at all. The warrant, not Google, specified the physical and temporal bounds of the geofence. The warrant authorized law enforcement, not Google, to narrow down the information to be disclosed at the warrant's second and third phase. Gov't Ex. 2 at 4. It is true that when a provider is directed to comply with a warrant, it has a due process right to challenge the warrant. *See, e.g.*, *In re Application*, 610 F.2d 1148, 1156-57 (3d Cir. 1979). But that possibility provides no evidence that the warrant was insufficiently particular.

In addition, the Fourth Circuit's decision in *McLamb* forecloses the defendant's argument that the warrant was facially deficient because its three-step process left too much discretion to

investigators. *See* Def. Post-Hr'g Suppl. Br. at 44. The defendant in *McLamb* argued to the Fourth Circuit that the Playpen warrant was insufficiently particular, in part because it allowed the FBI to "deploy the [search technique] more discretely against particular users." *See* Brief of Appellant at 46-47, *United States v. McLamb*, No. 17-4299 (available at 2017 WL 2832704). The Fourth Circuit relied on *Leon*'s good-faith exception to reject suppression, concluding that the Playpen warrant was not "so 'facially deficient ... that the executing officers [could not] reasonably presume it to be valid.'" *McLamb*, 880 F.3d at 691. Under *McLamb*, the warrant here was not facially deficient, even though it authorized investigators to obtain less evidence than they established probable cause for.

The defendant also claims that the issuing magistrate "abandoned his judicial role," but no evidence supports his claim. Def. Post-Hr'g Suppl. Br. at 41-42. The defendant begins by pointing out that the magistrate was relatively new to his job, but the defendant cites no law suggesting that *Leon* is somehow less applicable to a warrant issued by a new judge or magistrate. The defendant also notes that the magistrate spent 15 to 30 minutes reviewing the warrant application, but that was a sufficient length of time to read the relatively short affidavit and make a commonsense determination that there was a fair probability that Google possessed evidence of the bank robbery. The defendant further faults the magistrate for signing a warrant that the defendant claims lacked particularity, but as the United States has explained, the warrant specified its object with exacting particularity. *See supra* pages 37-40.

The Defendant concedes that he is "not making a *Franks* claim," but he then goes on to allege that the warrant application contained misleading information and material omissions. Def. Post-Hr'g Suppl. Br. at 45. Because he is not making a *Franks* claim, these allegations do not support an argument that the good-faith exception should not apply here. The United States notes,

however, that the defendant's allegations are incorrect. First, he claims that the information produced by Google in the first two steps was not anonymous, but in fact Google did not identify any individual until step 3, and additional research or information would have been required to identify an account owner. In the context of the language of the search warrant, that is what "anonymized information" means—the warrant stated that "anonymized information" was "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source." Gov't Ex. 2 at 4. Second, the defendant faults TFO Hylton for not informing the magistrate about Google's automated data filtering processes, but TFO Hylton lacked knowledge about Google's internal data structures. Suppresion Hr'g Tr. 606-67. Third, the defendant faults FBI TFO Hylton for not addressing potential inaccuracies in Google's location information. But the fact that there is some imprecision in cell phone location measurements is common knowledge; there is no reason FBI TFO Hylton would not have expected the issuing magistrate to be aware of that fact. In sum, the affidavit contained no misleading information, and any omissions were neither material to the issuance of the warrant, nor deliberate or reckless.

Finally, there is another more general reason why the investigators' reliance on the geofence warrant was reasonable: across the country, a broad array of neutral magistrates had approved geofence warrants, thus indicating their determinations that the warrants satisfy the Fourth Amendment. Magistrate Bishop's decision to sign the warrant was no outlier: Google received approximately 9000 geofence requests in 2019. Suppression Hr'g Tr. 489. FBI TFO Hylton himself had had geofence warrants approved by two state judges and a United States Magistrate Judge. Suppression Hr'g Tr. 603-04. And no judge had written an opinion rejecting an application for a geofence warrant. Given this context, and given FBI TFO Hylton's knowledge of other judges signing geofence warrants, FBI TFO Hylton's reliance on the geofence warrant in

this investigation was reasonable.

## III. CONCLUSION

For the reasons set forth in this brief, this Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

RAJ PAREKH
Acting United States Attorney

By: /s/

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov